DETAILED ACTION

This is a response to Applicant's Remarks and Amendments filed on August 18, 2008.

Claims 1, 2, 4, 7-11, 13, 14, 16, 19-25, 28, 29, 31, and 34-39 are currently pending.

Response to Amendment

The amendments to the Specification have been accepted.

Response to Arguments

1. Applicant's amendments to the Specification, see Amendments, filed August 18, 2008, with respect to claims 28, 29, 31, and 34-39 under 35 USC 101 have been fully considered and are persuasive. The rejections of these claims under 35 USC 101 have been withdrawn.

2. Applicant's arguments, see Remarks and Amendments, filed August 18, 2008, with respect to claims 1, 2, 4, 7-11, 13, 14, 16, 19-25, 28, 29, 31, and 34-39 under previously cited art by "Anonymous," Futa, Katsura, Boneh, and Eisentrager have been fully considered and are persuasive. The rejection of these claims has been withdrawn.

Allowable Subject Matter

1. Claims 1, 2, 4, 7-11, 13, 14, 16, 19-25, 28, 29, 31, and 34-39 are allowed.

The following is an examiner's statement of reasons for allowance:

The invention is directed to a public-private key cryptographic system wherein the keys correspond to an isogeny that maps a plurality of points from a first elliptic curve onto a second elliptic curve. Exemplary claim 23 provides for a public key that correspond to an isogeny and the decryption of an encrypted message is performed by using a decryption key corresponding to an isogeny using a bilinear pairing from a group

selected from Weil, Tate, and square pairings. Futa is the closest prior art found and is deficient in teaching the limitations set forth in claim 23.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MARTIN JERIKO P. SAN JUAN whose telephone number is (571)272-7875. The examiner can normally be reached on M-F 8:30a - 6:00p EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MJSJ/
Martin Jeriko San Juan
Examiner, Art Unit 2432

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2432